information

MDPI

Article

IPv6 Convergence for IoT Cyber–Physical Systems

Keith Nolan * and Mark Kelly

Intel Research and Development Ireland Limited, Leixlip W23 CX38, Ireland; mark.y.kelly@intel.com

* Correspondence: keith.nolan@intel.com; Tel.: +353-1-6066101

Received: 7 March 2018; Accepted: 22 March 2018; Published: 27 March 2018

check for updates

Abstract: We describe the evolution of the IoT towards a heterogeneous multitopology network subject to dynamic change and volatility yet still capable of secure and dependable operation. As part of this evolution, we outline the key changes in wireless communications technologies and heterogeneous networking that have arisen during the development of the IoT. We briefly outline the emerging area of cyber–physical systems, and associated technical challenges. We then describe how IP convergence can be viewed as the narrow waist connecting endpoint devices and fieldbus devices with applications and services in new Industry 4.0, and cyber–physical system use cases. We outline how a protocol-packing approach can be used for encapsulating LoRaWAN frames with IEEE 802.15.4 and IEEE 802.11 frames. Extending this, we propose a method for ultracompressed IPv6 signaling, and detail how this can be achieved in an example low-power wide-area technology, namely LoRaWAN. To support our proposed approach, we provide real-world analyses where IPv6 commands undergo a process of ultracompression and are then conveyed to a LoRaWAN endpoint. We find that IPv6 command ultracompression can potentially support command packet sizes that are over 20x smaller than the reported worst-case maximum protocol data unit size of 81 bytes.

Keywords: internet of things; low-power wide-area networking; internet protocol; LoRa; IPv6; cyber–physical systems

1. Introduction

The concept of the internet of things (IoT) has served as a precursor to what will likely lead to an evolved internet featuring decentralized adaptation, perceptive behaviors on a multiple-topology heterogeneous network infrastructure. Networking technology is evolving to a state that can enable anyone or anything to become a network operator and part of a global compute fabric. As a part of this evolution, networking is converging towards a common data and control plane approach.

Beyond the conventional IoT use cases, emerging cyber–physical systems targeting Industry 4.0 and connected vehicular systems will also require an unprecedented level of networking in the future. We envisage that networking comprising wireless and wired technologies will converge towards a single unifying encapsulation protocol, namely IPv6. We depict this convergence in Figure 1. Therefore, devising new methods to support IP control and data traffic on constrained networks, for example, low-power wide-area networking (LPWA) technologies, represents a significantly impactful research challenge.

Interconnecting heterogeneous networks and providing a service layer to support new applications and services is a critical ingredient in the evolving technology mix required to achieve these objectives. In Figure 2, we depict an example of multiple services operating in an overlay fashion on a heterogeneous network comprising a combination of WiFi, LPWA, cellular mobile and wireless mesh technologies. A converged IP layer on a heterogeneous network infrastructure is a necessary requirement to support the proliferation of future cyber–physical systems (CPS) targeted for new industrial/manufacturing and vehicular network use cases.

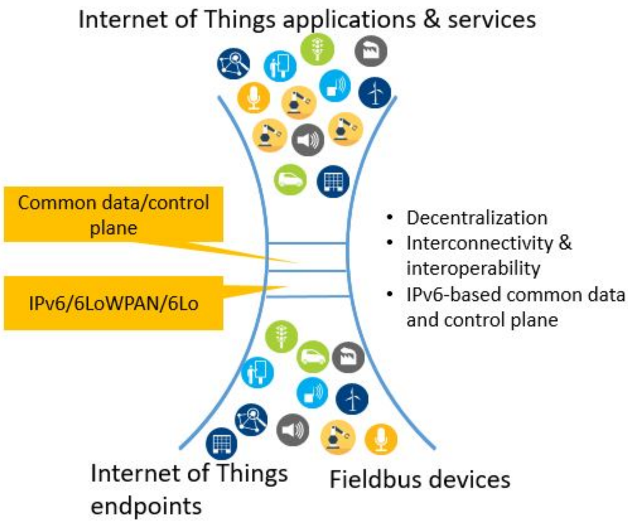

Figure 1. Convergence towards a common IPv6-based data and control plane connecting Internet of Things (IoT) endpoints and fieldbus devices with decentralised applications and services.

Figure 2. Complex multitopology heterogeneous WiFi, low power wide area (LPWA), mesh, and cellular networks with a common data and control plane supporting multiple different applications and services.

Cyber–Physical Systems

Cyber–physical systems (CPSs) are the seamless integration of compute, software (in the form of computational algorithms), and physical components such as embedded sensors, processors and actuators that are designed to sense and interact with the physical world. A CPS may be as simple as an individual device, or can consist of multiple cyber–physical devices that form a system, or can be a system of systems (SoS). Cyber–physical systems of systems (CPSoS) are generally large-scale systems that provide services that go beyond the services of any of their component CPSs. They also operate and are continuously evolving over long periods of time [1]. The actions of CPSs and constituent components must be both dependable and interoperable.

In Section 2, we provide a brief overview of wireless technologies commonly associated with IoT networks, with a particular focus on low-power wide-area networking. We then describe the motivation for adopting a converged IP approach, and follow up with our proposed model in Section 3. In Section 4, we detail our experimental approach used to explore an implementation of the model. We present initial findings in Section 5. Finally, we conclude in Section 6.

2. Background

We focus on the convergence of wireless technologies associated with the IoT and conventional enterprise networks. We propose a common data/control plane operating on an IP-interconnected hetnet comprising low power wide area (LPWA), IEEE 802.15.4 mesh, Ethernet, and wireless local area network (WLAN) technologies. Wireless technologies commonly associated with the IoT include IEEE 802.15.4 mesh [2], LoRaWAN [3], Sigfox [4], NB-IoT [5], Weightless-P [6], random-phase multiple access (RPMA) by Ingenu [7], and MIoTy from Fraunhofer-IIS [8], amongst others. In a previous work, we provided additional detail regarding the real-world performance of a selection of these wireless IoT networking technologies [9]. An example depicting LPWA and mesh is shown in Figure 3, where two non-IP technologies, LPWA and IEEE 802.15.4 mesh, are used as part of a WLAN- and Ethernet-based heterogeneous network. Our research focused on how we could enable these different systems to form a single connected layer abstracted from the underlying hetnet infrastructure, and upon which, support more services.

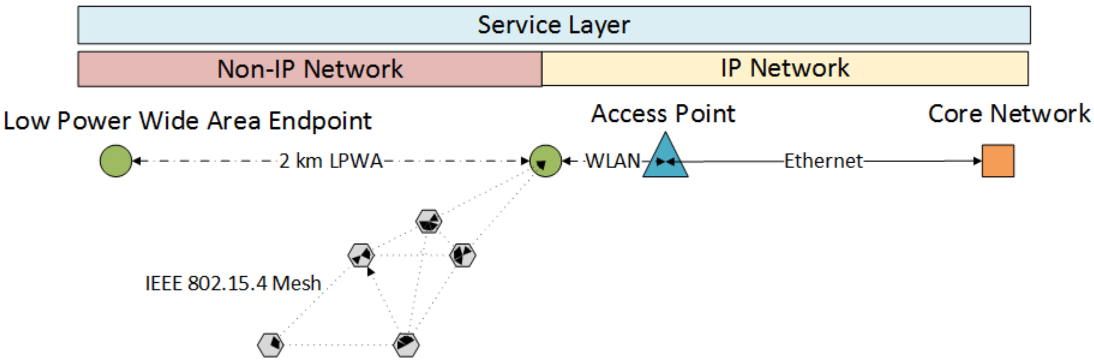

Figure 3. Interconnecting IP and Non-IP networks.

We briefly outline the following wired and wireless communications standards because they are already in use in the IoT but do not yet support an ability to interconnect with each other.

- **Ethernet**: IEEE 802.3 is a working group and a collection of IEEE standards produced by the working group defining the physical layer and data link layer's media access control (MAC) of wired Ethernet. Data rates range from 10 Mbps to 5GBASE-T (IEEE 802.3bz), 25 Gbps (IEEE 802.3by) and 400 Gbps (IEEE 802.3bs). This is generally a local area network technology used for core network backhaul with some wide-area network applications. Physical connections are made between nodes and/or infrastructure devices (hubs, switches, routers) by various types of copper or fiber cable.
- **EIA/TIA-485 (RS-485)**: The RS-485 standard was developed jointly by two trade associations: the Electronic Industries Association (EIA) and the Telecommunications Industry Association (TIA). The EIA once labeled all its standards with the prefix "RS" (Recommended Standard). Many engineers continue to use this designation, but the EIA/TIA has officially replaced "RS" with "EIA/TIA" to help identify the origin of its standards. It is a differential full duplex multipoint system supporting a maximum data rate of 10 Mbps up to a distance of 4000 ft [10].
- **IEEE 802.15.4:** IEEE 802.15.4 is a standard created and maintained by consultants which specifies the physical layer and media access control for low-rate wireless personal area networks (LR–WPANs). It is maintained by the IEEE 802.15 working group, which has defined it in 2003 [11].
- **IEEE 802.15.4g:** This is an amendment to IEEE Std 802.15.4-2011, where requirements for outdoor low-data-rate, wireless and smart-metering utility network requirements are addressed.
- **IEEE 802.11:** IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5 and 60 GHz frequency bands.

- **LTE Rel. 12+: NB-IoT**: Long Term Evolution (LTE) and LTE-Advanced [12,13] are 4th generation (4G) wireless communications standards designed to support low-latency (e.g., 5 ms at the user plane and 50 ms at the control plane) and high-bandwidth requirements (e.g., 50 Mb/s–1 Gb/s) between connected devices and the core network. From Release 12 onwards, Narrow Band IoT (NB–IoT) is supported. NB–IoT is a 3GPPP cellular technology for low-data-rate and low-power wide-area IoT networking. Frequency Division Duplexing (FDD) is used and the uplink and downlink bandwidth for a single NB–IoT carrier is 180 kHz [14]. Deployment options include standalone operation, within an existing LTE band, and/or within LTE guard bands. The MAC layer transport block size (TBS) can range from 2 bytes up to 125 bytes as specified by 3GPP TS36.213 [15]. IP support is dependent on TBS size due to the larger overhead associated with IP networking [16].
- **LoRaWAN:** LoRaWAN is low power wide area network specification intended for wireless-battery-operated IoT devices in regional, national or global deployments [3,17]. LoRaWAN targets key requirements for secure bidirectional communication, mobility and localization services. We detail the range of data payload capabilities in Appendix A [17,18].
- **SigFox:** SigFox created an ultra-narrowband IoT communications system designed to support IoT deployments over long ranges, for example, in excess of 20 km between a client device and a basestation [19]. This company has adopted an operator model, essentially creating a cellular network for IoT devices. Ultra-narrow-band operation is achieved using channel bandwidths of approximately 1 kHz that transport data payloads measured in tens of bytes. SigFox has targeted licence-exempt spectrum for their product, namely the 915 MHz band in the US and 868 MHz band in Europe. SigFox's model is a cloud-based approach where data are passed to the backend server and customer portal directly; users must then implement callbacks to route the received data to their own systems [19]. Sigfox does not support IP networking.
- **RPMA:** Random-phase multiple access (RPMA) is a bidirectional IoT communications technology developed by Ingenu that operates in the 2.4 GHz ISM band. Ingenu claim that RPMA coverage can extend up to 300 square miles, throughput of 19 kbps/MHz and an uplink link budget of 180 dB and 185 dB for downlink in the US. Citing security concerns, RPMA does not support IP connectivity. Instead, Ingenu choose to provide a REST API instead for data access [7].
- **WEIGHTLESS:** Weightless-P is a bidirectional communications technology that uses a combination of frequency-domain multiple access (FDMA) and time-domain multiple access (TDMA) operating using 12.5 kHz channel bandwidths. It was designed for use in the 169 MHz, 433 MHz, 470 MHz, 780 MHz, 868 MHz, 915 MHz and 923 MHz spectrum segments. It supports data rates from 200 bps to 100 kbps [6]. Two other variants are also available from the Weightless special interest group. Weightless-N is a unidirectional technology designed for 10-year operation using batteries with a 5 km+ range. Weightless-W was designed for 3–5 year operation using batteries but mainly targeted for use in "white space" spectrum, that is, generally described as the unused and available segments in the ultra-high-frequency band [20]. Neither of the Weightless variants support IP networking.
- **MIoTy:** Developed by Fraunhofer-IIS, MIoTy is a telegram-splitting multiple-access wireless technology requiring a bandwith of 200 kHz. It fragments data packets into numerous subpackets or telegrams, and distributes them over time and frequency. MIoTy was designed to support up to 15 km range in flat terrain, up to 65,000 messages per hour, 407 bits/s, have enhanced interference-resilience features for use in shared spectrum segments, for example, 868 MHz, 915 MHz ISM bands via the time- and frequency-distribution approach, and support mobility up to approximately 80 km/h [8]. MIoTy does not support IP connectivity.
- **IEEE 802.11af:** The IEEE 802.11af standard uses sub-1-GHz spectrum to extend broadband coverage to urban users. Unlike a cellular approach, this technology adopts a WLAN topology and was designed to use up to four bonded TV channels to achieve in excess of 400 Mbit/s data rates. This technology is better suited to neighbourhood WLAN-type deployments [21].

- **IEEE 802.11ah:** IEEE 802.11ah Task Group developed a new standard to address the particular requirements of M2M networks, which include a large number of power-constrained stations; a long transmission range; small and infrequent data messages; low data rates; and a non-critical delay. IEEE 802.11ah was designed to support 1 MHz and 2 MHz channels for the IoT and home automation services. However, it can increase this bandwidth to 4 MHz, 8 MHz or 16 MHz for larger data-rate requirements [22].

We group these technologies in terms of IP and non-IP support in Table 1.

Table 1. IP and non-IP classification

IP	Non-IP
IEEE 802.3 (Ethernet)	TIA/RS-485
IEEE 802.11 af/ah	IEEE 802.15.4 (without 6LoWPAN)
IEEE 802.15.4g	LoRAWAN
LTE Rel 12+/NB–IoT (transport block size dependent)	RPMA
	SigFox
	MIoTy

It is also important to outline the potential role of 5G-related activities and how they align with our vision of a converged IP networking future.

2.1. 5G Ecosystem Context

In July 2016, the 5G Public Private Partnership (5GPPP) Architecture Working Group published a whitepaper regarding their view of 5G architecture [23]. They depicted a 5G ecosystem where infrastructure and network function layers are two distinct separate entities. In July 2016, it was reported that Verizon became the first US carrier to complete its own 5G specification [24,25]. As part of this, Verizon's 5G Network and Signaling Working Group published a 5G packet convergence protocol where they detail the services provided to upper layers comprising data transfer and radio resource allocation supporting a maximum protocol data unit (PDU) size of 65528 octets [26]. In a previous work, we also described how 5G also represents convergence of wireless technologies also [27].

It is intended that these PDUs transport IP packets [28] using a structure comprising the physical layer (PHY), medium access control (MAC), radio link control (RLC), and a packet data convergence protocol (PDCP) layer. The IP connectivity connection point is at the PDCP layer as depicted in Figure 4. 5G is intended to be a flat IP network and this is one of the key features needed make 5G acceptable for broad adoption and support for internet of the future technologies.

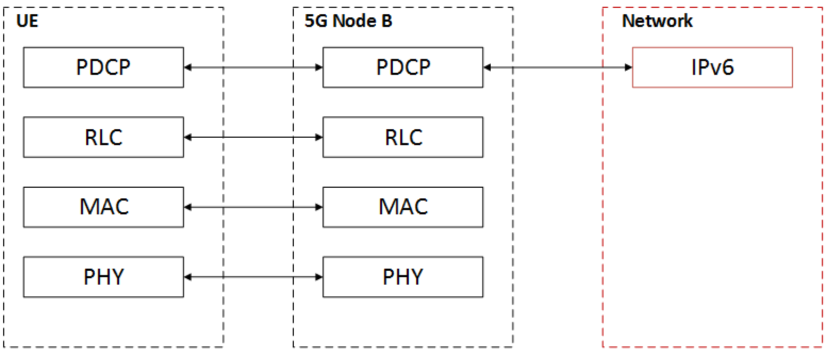

Figure 4. 5G architecture stack outline comprising a physical layer (PHY), medium access control (MAC) layer, radio link control (RLC) layer and a packet data convergence protocol (PDCP) layer. IPv6 packets would flow between the networking layer and the Packet Data Convergence Protocol layer, which we depict in red in this diagram.

Opportunities exist to extend the 5G network function layer vision where interconnectivity, interoperability and in-network computation requirements present critical research challenges specifically in the massive machine-type communications (mMTC) and critical machine-type communications (uMTC) areas. As depicted in Figure 1, our view of 5G is that IPv6/6LoWPAN over PDCP will also be the common convergence layer between the underlying heterogeneous compute and communications technologies and the applications and services of the internet of the future (IoTF).

CPS and advanced IoT networks are trending towards a heterogeneous network future also. This introduces a new set of technical challenges, particularly when the network may be dynamic and volatile in nature. We now outline some of the key research focusing on these aspects.

2.1.1. Heterogeneous Networks

Two key challenges involved in managing a dynamic wireless communications infrastructure involving mobile nodes are the increased computational load and network propagation delays. Chakrabarti and Mishra investigated the challenge of quality of service (QoS)-based routing with incomplete network state information in 2001 [29]. They focused on mobile nodes without a fixed infrastructure interconnected by multihop communication paths with dynamically changing topologies. They summarised that guaranteeing QoS in such a network where nodes join and leave the network, and incomplete network state information exists, may be impossible if nodes are too mobile. In 2002, Park, Savvides and Srivastava developed a set of NS-2 simulation models and techniques mainly focusing on a sensing channel through which sensors detect targets, and provided detailed models for evaluating energy consumption and battery lifetime [30]. The concept of abstracting services or dataflow away from the underlying infrastructure in a wireless sensor network context was initially addressed in some detail by Aberer, Hauswirth and Salehi in 2007 [31]. They proposed a global sensor network middleware supporting dynamic integration and management of distributed sensor networks and a virtual sensor which abstracts from implementation details. This virtual sensor concept is essentially a container with the ability to accept multiple inputs, produce one output data stream, and include all necessary metadata required for deploying and using it. However, this approach is high level; it uses eXtensible Markup Language (XML) to describe the sensors and Structured Query Language (SQL) to deal with query execution.

In 2011, Akribopoulos et al. proposed a platform-agnostic framework for integrating heterogeneous smart objects in the Web of Things [32]. Their framework consisted of four different hardware platforms, Arduino, SunSPOT, TelosB and iSense. The authors described the necessary steps required to make such a heterogeneous network interoperate, in the form of a software library, named mkSense, that enables their intercommunication. They describe the design and implementation of a software library that can be used for building "intelligent software" for the Web of Things. The authors focused on interconnecting different IEEE 802.15.4-based systems to create their heterogeneous sensor network. The first step was to set all the devices to 16-bit addressing mode, and to the same personal area network (PAN) ID and channel. Following this, they built a library for each of the devices we wanted to support, which were intended to care for on-boot device configuration involving resource initialization for IEEE 802.15.4 communication and exposing an application programming interface (API) for users.

Our summary of this work is that without sufficient network state knowledge, the underlying algorithmic complexity involved in determining optimal routing strategies may be perceived as intractable, that is, NP-complete. In order for us to sufficiently address this challenge, guided assumptions regarding the network state and topology may be required to devise strategies within a constrained time window. It can be argued that adopting a converged IP approach for heterogeneous networks significantly reduces or potentially eliminates the problem of multiple siloed networks and inefficient use of combined networking resources as a result.

2.2. The Path Towards IP Convergence

The potentially many different permutations of IP and non-IP network infrastructure types coupled with requirements to support a multitude of services necessitate a design where IP to non-IP translation and interconnection does not require dedicated translation nodes and in fact, can be dynamically triggered on demand. Dynamic interconnection is valuable for dealing with volatile IoT infrastructure where nodes can both join and leave networks and may be mobile. We show an example of a hetnet infrastructure in Figure 5, where IP to non-IP interconnectivity is required at multiple stages and where a plurality of services require support.

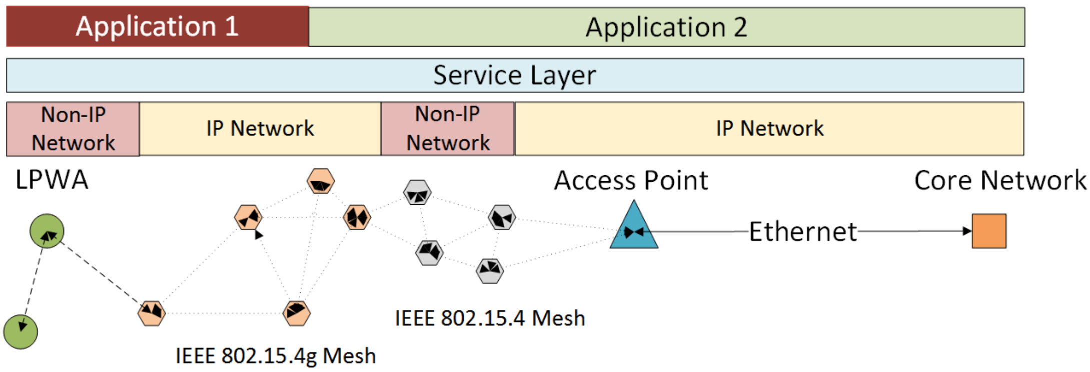

Figure 5. Multiple interconnecting IP and Non-IP networks supporting one or more services.

Our research focused on the extension of IP support to communications technologies where native IP support was not currently available. We target LoRAWAN in particular. Existing academic research regarding IPv6 over LPWA is very limited. In 2017, Thielemans et al. proposed doing this by replacing the LoRaWAN MAC protocol with the Contiki networking stack [33]. In 2016, Weber et al. proposed an approach analogous to the standardized and established 6LoWPAN protocol where IPv6 is adapted via header compression and field eliding to IEEE 802.15.4. In this case, they proposed adopting a similar approach for LoRaWAN; a scheme they named 6LoRaWAN [34]. However, our proposed approach was extended to reduce IPv6/6LoWPAN overhead even further and generalised to extend over additional communication technologies.

3. IP-Convergence Model

Our IP-convergence model approach focused on IPv6 over a low-power wireless personal area network (6LoWPAN) as a baseline, which we extended further for ultracompressed IPv6 signaling.

3.1. 6LoWPAN

6LoWPAN is an adaptation header format. It enables the use of IPv6 over low-power wireless links. It features IPv6 and UDP header compression. The format was initially defined in RFC4944 and updated by RFC6282. It originally was designed for low-power wireless personal area networks (LoWPANs) comprising devices that conformed to the IEEE 802.15.4-2003 standard. The main characteristics of 6LoWPAN are that it supports small packet sizes, 16-bit short or IEEE 64-bit extended media access control addresses and low-to-medium bandwidth (250/40/20 kbps). Star and mesh network topologies are supported; networks are generally ad hoc, and devices have limited accessibility and user interfaces. The intended use cases predominately feature devices requiring low-power battery-operated modes and are relatively low cost. It was also designed for networks that are inherently unreliable due to nature of devices in the wireless medium.

3.1.1. Challenges

6LoWPAN also presents a number of challenges. Specifically, IP support over IEEE 802.15.4 networks is not trivial; the worst-case 802.15.4 protocol data unit (PDU) size is 81 octets, whereas IPv6 maximum transmission unit (MTU) requires 1280 octets [35]. Stacking IP and above layers "as is" may not fit within one 802.15.4 frame; for example, IPv6 40 octets, TCP 20 octets, UDP 8 octets and other layers (security, routing, etc.) can result in a large overhead.

Not all ad-hoc routing protocols may be immediately suitable for LoWPAN. Dynamic source routing (DSR) may not fit within a packet. Ad-hoc on-demand distance vector (AODV) requires increased memory support. Current service discovery methods are considered too heavyweight for LoWPAN. In order to support seamless IoT deployments, limited configuration and management overhead are attractive features. Security for multihop networks is a critical requirement also. Regarding performance of large IPv6 packets, fragmentation over low-power wireless mesh networks may lead to poor performance especially in lossy energy-constrained networks where packet losses are frequent. Lost fragments can cause the whole packet to be retransmitted rather than the missing fragments. Low-bandwidth and wireless channel behavior, for example, delay, must be accounted for when preparing data for dispatch, that is, pre-processing or data distillation is an important consideration for maximising networking efficiency.

The LoWPAN IP header compression (LoWPAN_IPHC) encoding format was developed for effective compression of unique local, global and multicast IPv6 addresses based on shared state within contexts. When routing over multiple IP hops, LOWPAN_IPHC can compress the IPv6 header down to 7 octets. This frame structure, depicted in Figure 6, comprises:

- 1-octet Dispatch
- 1-octet LOWPAN_IPHC
- 1-octet Hop Limit
- 2-octet Source Address
- 2-octet Destination Address

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Dispatch   |      IPHC     |   Hop Limit   | Source Address|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               |      Destination Address      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6. Compressed IPv6 header.

In our proposed approach, we also explored how fragmentation and worst-case protocol data-unit-size challenges could be addressed. In particular, our key design considerations were as follows:

1. How could we support at least a PDU size of 81 octets to meet the worst-case 6LoWPAN PDU size requirement?
2. How can we support multi-hop networks?
3. What new research was needed to address PDU size support for less than 81 octets to enable IPv6 support on highly constrained networking technologies?

3.2. LoRaWAN

For the purposes of our research and as a representative candidate of a technically challenging technology that does not natively support IP networking, we focus on LoRaWAN. LoRaWAN is a popular low-power wide-area wireless networking technology using a protocol defined by the LoRa Alliance and formalised in the LoRaWAN specification [3,17]. It uses a chirp-spread or frequency shift keying (FSK) modulation scheme and is primarily targeted to the industrial, scientific and medical (ISM) radio bands. It is designed to support medium-to-long-range communications between energy-constrained wireless nodes and gateways, which operate in conjunction with backend network and application servers. LoRaWAN has three modes of operation; Modes A, B and C. In Mode A, endpoint devices initiate upstream messages and may open receive windows one and two seconds following transmission for receipt of downstream acknowledgements and/or additional MAC instructions, for example, for adaptive data-rate control. In Mode B, endpoints may receive beacons from gateways in addition to the Mode A functionality. In Mode C operation, endpoint devices may continuously receive frames when not transmitting messages.

In our experimentation, we focused on Mode A operation, but our proposed approach can easily be adapted for use in other modes. In fact, we argue that achieving IP networking in LoRaWAN Mode A is the more technically challenging option as the endpoint must initiate messaging first and can only receive downstream messages during one or both of the subsequent receive windows following transmission.

3.3. IPv6 over LoRaWAN

We now consider how IPv6 over LoRaWAN can be supported. The LoRaWAN specification details the range of maximum payload sizes supported for both the US and European variants. In this study, we primarily examine the European 863–870 MHz and 915 MHz US cases initially. Our starting point is identifying how the reported worst-case 6LoWPAN PDU size can be supported by LoRaWAN when considering EU863–870 MHz and US915 MHz cases for both no-repeater-compatible and repeater-compatible modes of operation. We detail the maximum payload sizes for the data-rate range supported for EU863-870 MHz for both no-repeater and repeater-compatible cases in Table A4 and Table A3, respectively. We present the same metrics for US915 MHz for both no-repeater and repeater-compatible use cases in Tables A1 and A2, respectively. For the reported worst-case PDU size, we find that eight of the eleven defined data rates for both of the repeater-compatible and no-repeater configurations could support the worst-case PDU size. We outline these in Table A6 (EU863-870 MHz no-repeater), Table A5 (EU863-870 MHz repeater compatible), Table A8 (US915 MHz no repeater), and Table A7 (US915 MHz repeater compatible).

Recalling the initial challenge of supporting the worst-case PDU size of 81 octets for 6LoWPAN, we note that LoWPAN_IPHC can compress the IPv6 header down to 7 octets, and therefore, we can potentially support smaller PDU sizes than the worst-case PDU length of 81 bytes. We propose an ultracompressed method to achieve this for all LoRaWAN data-rate options.

4. Proposed Approach

Our proposed approach is based on the idea of encapsulating one protocol within another. We further extended this by introducing a method of instruction and data compression to reduce the overhead even further.

4.1. Protocol Packing

We use the term protocol packing to denote the process of packing one protocol frame inside the payload field of another protocol frame. By adopting this approach, both protocols remain standards-compliant. An example is depicted in Figure 7, where a LoRaWAN frame is packed into the payload field of an IEEE 802.15.4 MAC frame. In this example, the entire LoRaWAN radio PHY frame comprising the preamble, PHY header, cyclic redundancy check (CRC), PHY payload, and frame CRC (for uplink messages only), is simply encapsulated into the MAC payload of an IEEE 802.15.4 frame. Following the pre-pending of the IEEE 802.15.4 MAC header and appending the MAC footer, the hybrid payload is then used as the PHY payload for the complete IEEE 802.15.4 frame.

A similar approach can be adopted for packing LoRaWAN frames inside IEEE 802.11 frames. We outline this process in Figure 8. In this example, the complete LoRaWAN frame is encapsulated within the network data field of the IEEE 802.11 MAC frame.

Other data link layer and transport encapsulation targets can be supported using this method. Examples include, and are not limited to, Data Over Cable Service Interface Specification (DOCSIS) [36] and AX.25 [37]. DOCSIS is used for high-data-rate transfer over cable and wireless systems. It is predominately used for high-data-rate transfer, for example, broadband internet and television services. AX.25 was developed by the Tucson Amateur Packet Radio (TAPR) and American Radio Relay League (ARRL) organisations in 1996 with an update in 1998. This is a data-link layer protocol derived from the X.25 protocol and was primarily designed for use in impaired narrowband wireless networks, predominately in the amateur radio bands.

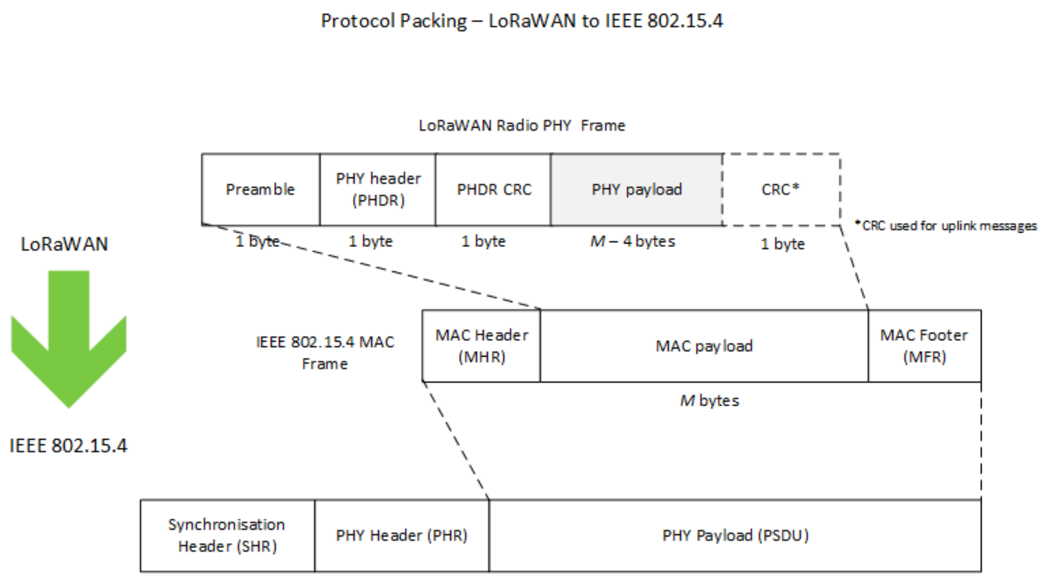

Figure 7. Packing LoRaWAN frames inside an IEEE 802.15.4 MAC frame.

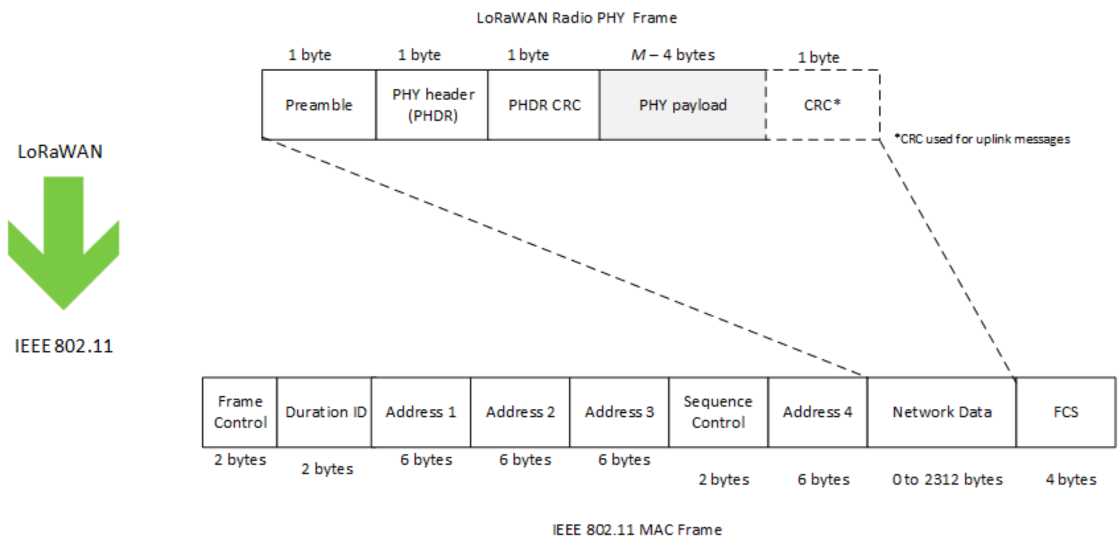

Figure 8. Packing LoRaWAN frames inside an IEEE 802.11 MAC frame.

In our approach, we do not simply encapsulate protocol frame data within the payload field of another protocol; we include additional field eliding and command compression. However, our proposed approach also introduces new challenges, requiring additional research. These include the management of complex fragmentation and defragmentation as a result of reducing the worst-case PDU size below 81 bytes and restricted payload sizes (due to the protocol packing overhead). In addition, the number of packed protocols arising from use within heterogeneous networks may be limited, and the number of interconnections supported is strongly linked to the specific hetnet topology under investigation and requires additional extensive research to fully characterise.

4.1.1. Fragmentation Strategy

We extended the baseline fragmentation strategy set out in Internet Engineering Task Force (IETF) 6LoWPAN. In the baseline strategy, if a datagram does not fit within the size of a single IEEE 802.15.4 frame, it is broken into link fragments. The fragment offset can only express multiples of eight bytes, and therefore, all link fragments for a datagram except the last one must be multiples of eight bytes in length. The first link fragment contains the first fragment header defined, as shown in Figure 9.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  11000  |     Datagram Size     |          Datagram Tag         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 9. First fragmentation header.

The second and subsequent fragmentation header is shown in Figure 10.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  11000  |     Datagram Size     |          Datagram Tag         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Datagram Offset|
+-+-+-+-+-+-+-+-+
```

Figure 10. Second and subsequent fragmentation header.

The frame fields are as follows:

- **Datagram_size:** This 11-bit field encodes the size of the entire IP packet before link-layer fragmentation (but after IP-layer fragmentation).
- **Datagram_tag:** The value of datagram_tag (datagram tag) shall be the same for all link fragments of a payload.
- **Datagram_offset:** This field is present only in the second and subsequent link fragments and specifies the offset, in increments of 8 octets of the fragment from the beginning of the payload datagram.

4.2. IPv6 over LoRaWAN

If the worst-case PDU size of 81 bytes was adopted, then a protocol-packing approach can potentially support five of the eight defined data rates for both of the repeater-compatible and no-repeater configurations. We can therefore summarize as follows:

- As a concept, protocol packing appears a feasible approach of encapsulating 6LoWPAN PDUs in existing US and EU LoRaWAN payloads.
- Protocol packing is potentially a method to preserve standards/alliance compliance.
- For maximum usage efficiency of the underlying communications technology, we still need to develop methods to support 6LoWPAN PDUs for the lowest LoRaWAN data rates; for example, for 19-, 59- and 61-octet payloads.

In our work, however, we examined how to support IP connectivity for all LoRaWAN maximum-payload-size options and then further extended this to create an ultracompressed IP-control messaging approach. Our protocol-packing design approach is illustrated in Figure 11, and the steps are as follows:

1. Perform command compression and additional field eliding. Copy the 6LoWPAN PDU frame into the frame payload field of the LoRaWAN MAC payload data structure.
2. Insert this MAC payload into the LoRaWAN PHY payload frame field.
3. Map the PHY payload frame into the LoRaWAN radio frame.
4. The LoRaWAN frame is ready for dispatch.

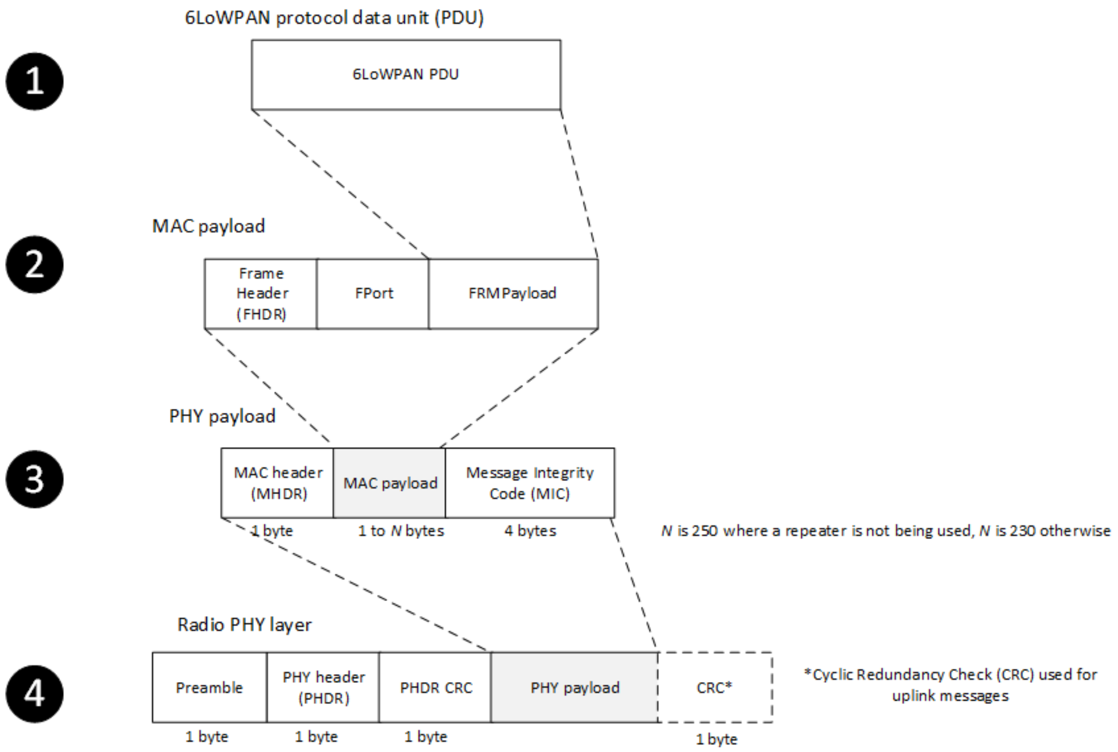

Figure 11. Packing 6LoWPAN as LoRaWAN frames.

The key stages of our proposed ultracompression method are as follows. The normal IPv6 header, depicted in Figure 12, comprises 40 bytes.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic Class |           Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |  Next Header  |   Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                         Source Address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Destination Address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 12. IPv6 header format.

The ICMPv6 header comprises four bytes with an optional data field (Figure 13).

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                          Message Body                         +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 13. ICMPv6 header format.

The initial ICMPv6 information request/response used for testing was an echo request, which comprises the frame format shown in Figure 14.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Identifier          |        Sequence Number        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                              Data                             +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 14. ICMPv6 echo request packet format.

We combined the 6LoWPAN approach outlined in Section 4.1.1, Robust Header Compression (RoHC) compression [38] and field eliding, for example, and the data field was not required, as a means of producing an ultracompressed ICMPv6 packet ready for use with LPWA networks. The header format following initial RoHC compression is described in Figure 15.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|t|n| hl|c|s|sam|m|d|dam|
+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 15. RoHC IPv6 header frame format.

Further compression was made possible by extending a LPWA network server to maintain an active cache of endpoint addresses and states, and performing address translation at that point. In addition, for ICMPv6-like control messages, the command code length is fixed, and therefore, further field eliding was possible; for example, payload length eliding. As a result, we could compress the header to one byte. As an example, following additional field eliding, we created a frame format supporting ultracompressed IPv6 ICMPv6 commands in Figure 16.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Header    |      Code     |    Checksum   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 16. Ultra-compressed IPv6 ICMPv6 message for LoRaWAN.

The sequence of transactions required to support the dispatch of 6LoWPAN PDUs from an IPv6 node to an IPv6 node via a LoRaWAN hetnet is depicted in Figure 17.

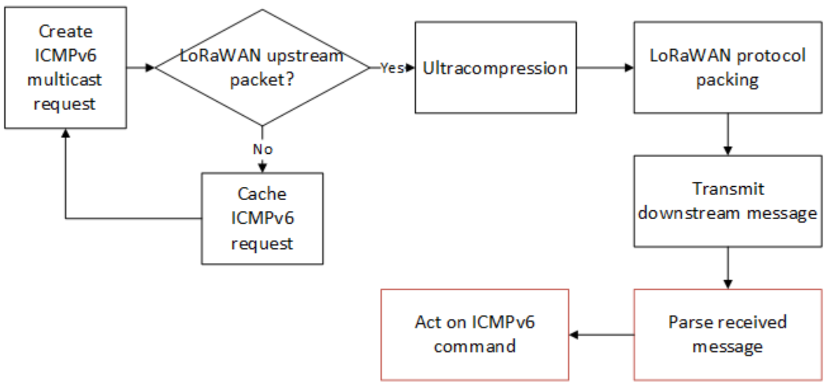

Figure 17. Main processes involved for the downstream handling of ICMPv6 commands and LoRaWAN messaging.

5. Evaluation and Results

Our experimental configuration, depicted in Figure 18, comprised a LoRaWAN endpoint, a gateway node, a LoRaWAN network server and a test client device capable of issuing IPv6 ICMPv6 requests. The LoRaWAN endpoint operated in the 868 MHz ISM band and was configured for Mode A operation with confirmed upstream messages. Our LoRaWAN gateway was connected to a network server via Ethernet. Our test IPv6 clients also connected to the network server via Ethernet. Multicast IPv6 requests were compressed and routed to the LoRaWAN endpoint via this network server. A basic example of a multicast request is an echo request. We also conducted testing using the private experimentation fields (200, 201) as defined in RFC4443 [39].

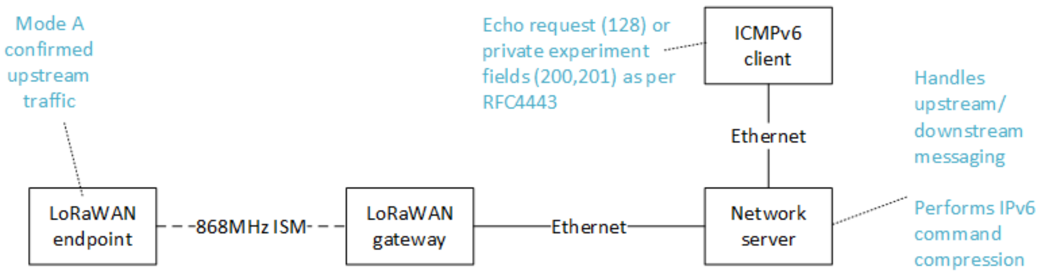

Figure 18. Experimental configuration—we used the 868 MHz industrial, scientific, and medical (ISM) radio band with LoRaWAN Mode A and confirmed upstream traffic.

The ICMPv6 request and downstream messaging process via LoRaWAN is depicted in Figure 17. In this example, the ICMPv6 request handling and compression and LoRaWAN messaging are connected processes, and the stages performed by the endpoint are outlined in red. The network server was responsible for performing caching and compression of incoming multicast ICMPv6 commands and waiting for LoRaWAN upstream messages before appending the compressed commands to the downstream ACKs.

In Figure 19, we provide an excerpt from the network server log where an upstream message has been received. The cached compressed ICMPv6 command, which was targeted for that specific LoRaWAN endpoint, is appended to the downstream ACK. In this example, the compressed IPv6 header, command and checksum octets are `0xC0 0xA1 0x61`, respectively.

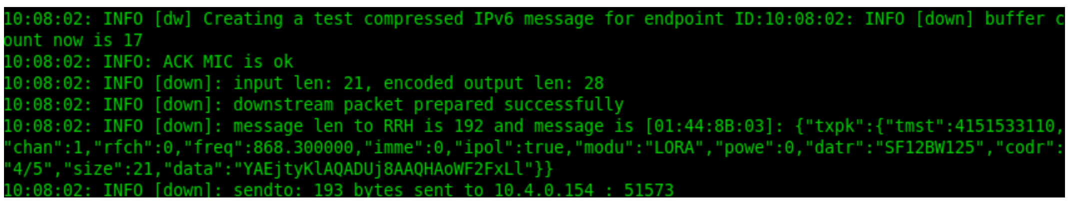

Figure 19. LoRaWAN network server reports an upstream message.

Following this, Figure 20 is an excerpt of the LoRaWAN gateway log where the downstream packet has been scheduled for transmission, targeting the first receive window for the endpoint. The three bytes comprising the compressed ICMPv6 command have been appended to the LoRaWAN MAC frame field, as highlighted in this figure.

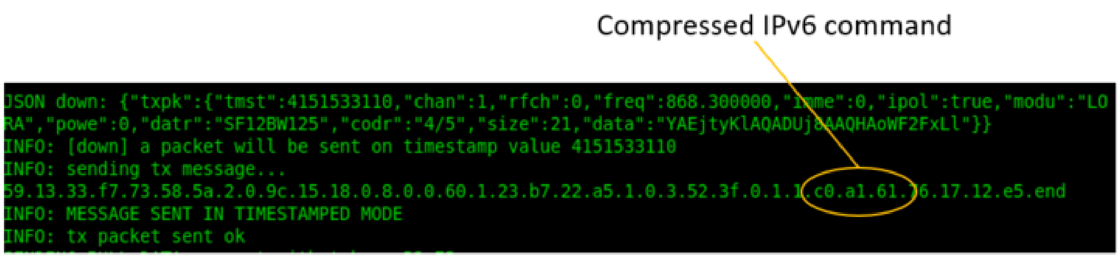

Figure 20. We prepare a LoRaWAN ACK containing a 3-byte ultracompressed IPv6 command, which is transmitted by the LoRaWAN gateway.

In Figure 21, we depict a spectrogram showing the upstream message from the test endpoint and ACK waveform, with the appended compressed ICMPv6 command from the LoRaWAN network server one second later.

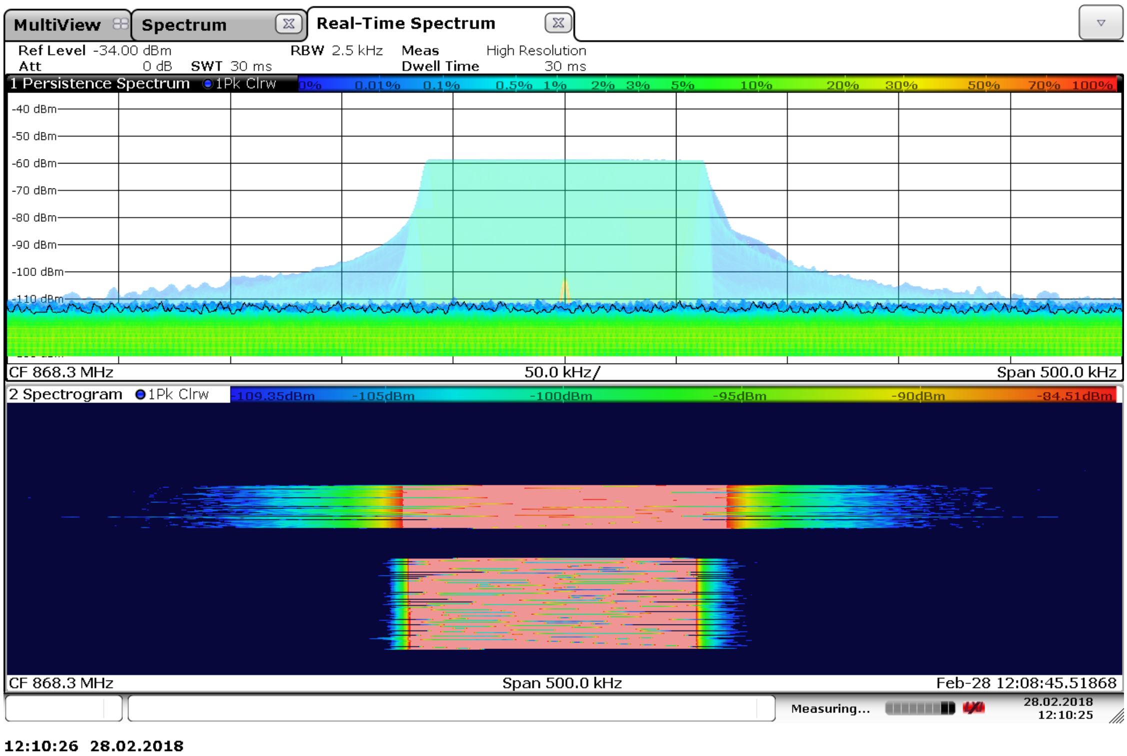

Figure 21. A spectrogram depicting the upstream message and ACK from the LoRaWAN network server one second later.

In Figure 22, we present an excerpt from the LoRaWAN test endpoint indicating the received downstream message, and we highlight the received command structure within the downstream message.

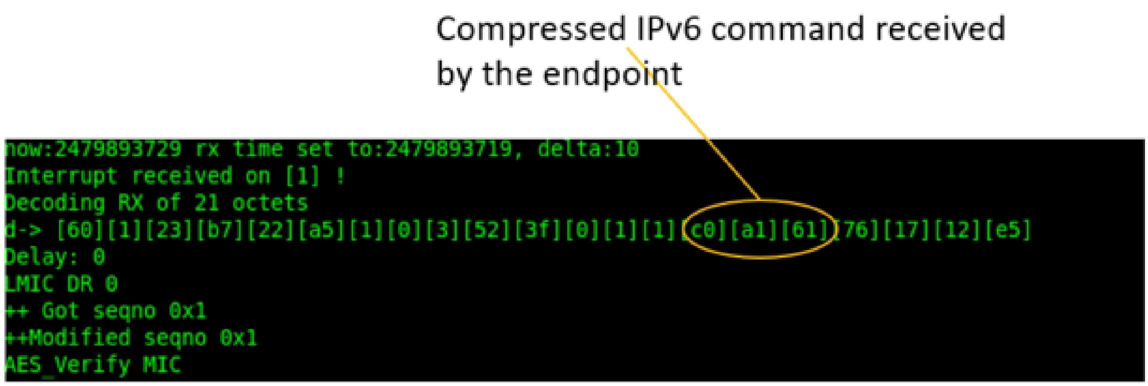

Figure 22. Received downstream bytes reported by a LoRaWAN test endpoint.

Through this initial experimentation, we were able to determine that IPv6 commands via further compression of 6LoWPAN for support over very constrained networks is feasible. Our initial findings based on LoRaWAN experimentation, and outlined in Table 2, indicated that we could dispatch and receive ultracompressed IPv6 commands that were 27x smaller than the reported maximum PDU (or MTU) size of 81 bytes.

Table 2. IPv6 command compression.

Scheme	Packet Size (bytes)	Compression Factor
IPv6 worst-case PDU	81	
Proposed approach	3	27

6. Conclusions

In this article, we described the evolution of the IoT towards a heterogeneous multitopology network subject to dynamic change and volatility yet still capable of dependable operation. As part of this evolution, we outlined the key changes in wireless communications technologies that have arisen during the development of the IoT. We then adopted an IP-convergence view and outlined how this can be viewed as the narrow waist connecting endpoint devices and fieldbus devices with applications and services in new Industry 4.0 and cyber–physical system use cases. We outline how a protocol-packing approach could be used for encapsulating LoRaWAN frames with IEEE 802.15.4 and IEEE 802.11 frames. We then proposed an ultracompressed IPv6 signaling approach and detailed how this could be achieved in an example low-power wide-area technology, namely LoRaWAN. To support our proposed approach, we provided real-world analyses where IPv6 commands underwent a process of ultracompression and were then conveyed to a LoRaWAN endpoint. Our initial findings indicated that ultracompressed IPv6 commands that are over 20× smaller than the reported maximum PDU (or MTU) size of 81 bytes can be supported.

Author Contributions: Keith Nolan and Mark Kelly wrote the article.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ACK	Acknowledgment
AODV	Ad-hoc on-demand distance vector
CPS	Cyber–physical system
CRC	Cyclic redundancy check
DSR	Dynamic source routing
EIA	Electronic Industries Association
ICMPv6	Internet Control Message Protocol version 6
IETF	Internet Engineering Task Force
IoT	Internet of things
IPv6	Internet Protocol version 6
LPWA	Low-power wide-area networking
MAC	Medium access control
M2M	Machine to machine
MTU	Maximum transmission unit
NB–IoT	Narrow-band internet of things
PAN	Personal area network
PHY	Physical layer
PDCP	Packet Data Convergence Protocol
PDU	Protocol data unit
RLC	Radio link control
RPMA	Random-phase multiple access
SQL	Structured Query Language
TIA	Telecommunications Industry Association
TBS	Transport block size

XML	eXtensible Markup Language
3GPPP	3G Public Private Partnership
5GPPP	5G Public Private Partnership
6LoWPAN	IPv6 over low-power wireless personal area network

Appendix A. Tables of LoRa Maximum Payload Sizes

US915 MHz Operation [3].

Table A1. Maximum payload sizes for US915MHz repeater-compatible operation.

Maximum Payload Sizes (US)—Repeater Compatible		
Data Rate	**MAC Payload Length**	**MAC Control Field Length**
0	19	11
1	61	53
2	137	129
3	250	242
4	250	242
5:7	Not defined	
8	41	33
9	117	109
10	230	222
11	230	222
12	230	222
13	230	222
14:15	Not defined	

The maximum payload sizes for cases where a repeater will not be used are as follows [3].

Table A2. Maximum payload sizes for US915MHz repeater-incompatible operation.

Maximum Payload Sizes (US)—Not Repeater Compatible		
Data Rate	**MAC Payload Length**	**MAC Control Field Length**
0	19	11
1	61	53
2	137	129
3	250	242
4	250	242
5:7	Not defined	
8	61	53
9	137	129
10	250	242
11	250	242
12	250	242
13	250	242
14:15	Not defined	

For EU 863-870 MHz operation, the maximum payload sizes are as follows [3].

Table A3. Maximum payload sizes for EU863-870MHz repeater-compatible operation.

Maximum Payload Sizes (EU)—Repeater Compatible		
Data Rate	**MAC Payload Length**	**MAC Control Field Length**
0	59	51
1	59	51
2	59	51
3	123	115
4	230	222
5	230	222
6	230	222
7	230	222
8:15	Not defined	

Table A4. Maximum payload sizes for EU863-870MHz repeater-incompatible operation.

Maximum Payload Sizes (EU)—Not Repeater Compatible		
Data Rate	**MAC Payload Length**	**MAC Control Field Length**
0	59	51
1	59	51
2	59	51
3	123	115
4	250	242
5	250	242
6	250	242
7	250	242
8:15	Not defined	

For EU operation, the maximum payload sizes supporting the worst-case PDU sizes are as follows [3].

Table A5. Maximum payload sizes for EU863-870MHz repeater-compatible operation supporting the 81-byte worst-case PDU limit.

Maximum Payload Sizes (EU)—Repeater Compatible		
Data Rate	**MAC Payload Length**	**MAC Control Field Length**
3	123	115
4	230	222
5	230	222
6	230	222
7	230	222

Table A6. Maximum payload sizes for EU863-870MHz repeater-incompatible operation supporting the 81-byte worst-case PDU limit.

Maximum Payload Sizes (EU)—Not Repeater Compatible		
Data Rate	**MAC Payload Length**	**MAC Control Field Length**
3	123	115
4	250	242
5	250	242
6	250	242
7	250	242

For US 915 MHz operation the maximum payload sizes supporting the worst-case PDU sizes are as follows [3].

Table A7. Maximum payload sizes for US915 MHz repeater-compatible operation supporting the 81-byte worst-case PDU limit

Maximum Payload Sizes (US)—Repeater Compatible		
Data Rate	**MAC Payload Length**	**MAC Control Field Length**
2	137	129
3	250	242
4	250	242
9	117	109
10	230	222
11	230	222
12	230	222
13	230	222

Table A8. Maximum payload sizes for US915 MHz repeater-incompatible operation supporting the 81-byte worst-case PDU limit.

Maximum Payload Sizes (US)—Not Repeater Compatible		
Data Rate	**MAC Payload Length**	**MAC Control Field Length**
2	137	129
3	250	242
4	250	242
9	137	129
10	250	242
11	250	242
12	250	242
13	250	242

References

1. CPSoS Project. *D2.4 Analysis of the State-of-the-Art and Future Challenges in Cyber-Physical Systems of Systems*; European Union: Brussels, Belgium, 2013.
2. LAN/MAN Standards Committee. *ANSI/IEEE 802.15.4–2006—IEEE Standard for Information Technology—Local and Metropolitan Area Networks—Specific Requirements—Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)*; IEEE Standards Association: New York, NY, USA, 2006; Volume 2006, p. 323.
3. LoRa Alliance. LoRa-Alliance | LoRaWAN for Developers. Available online: https://www.lora-alliance.org/lorawan-for-developers (accessed on 26 March 2018).
4. Sigfox. *Sigfox Technology Overview*; Sigfox: Labège, France, 2016.
5. Huawei. *NB-IOT White Paper*; Huawei: Shenzhen, China, 2015.
6. Webb, W. *Weightless: A Bespoke Technology for the IoT*; Technical Report; Weightless: Cambridge, UK, 2013. Avaliable online: http://www.weightless.org/news/weightless-a-bespoke-technology-for-the-iot (accessed on 26 March 2018).
7. Ingenu. *How RPMA Works: The Making of RPMA*; Ingenu: San Diego, CA, USA, 2016; p. 92.
8. Fraunhofer IIS. *MIOTY—The Wireless IoT Platform*; Fraunhofer IIS: Munich, Germany, 2018. Available online: http://mioty.de/(accessed on 26 March 2018).
9. Nolan, K.E.; Guibene, W.; Kelly, M.Y. An evaluation of low power wide area network technologies for the Internet of Things. In Proceedings of the 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, Cyprus, 5–9 September 2016; pp. 439–444.
10. Maxim Integrated Products. *RS-485 (EIA/TIA-485) Differential Data Transmission System Basics—Tutorial*; Maxim Integrated Products: San Jose, CA, USA, 2001.

11. IEEE Standards Association (IEEE SA). *IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks*; IEEE SA—802.15.4g-2012; IEEE SA: Piscataway, NJ, USA, 2012.
12. Ghosh, A.; Ratasuk, R. *Essentials of LTE and LTE-A*; Cambridge University Press: Cambridge, UK, 2011; pp. 1–249.
13. Parkvall, S.; Dahlman, E.; Furuskär, A.; Jading, Y.; Olsson, M.; Wänstedt, S.; Zangi, K. LTE-Advanced—Evolving LTE towards IMT-Advanced. In Proceedings of the IEEE Vehicular Technology Conference, Calgary, BC, Canada, 21–24 September 2008.
14. Beyene, Y.D.; Jantti, R.; Ruttik, K.; Iraji, S. On the performance of narrow-band internet of things (NB–IoT). In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA, 19–22 March 2017.
15. Teesside Small Gauge Railway. *TS 136 213—V13.0.0—LTE: Evolved Universal Terrestrial Radio Access (E-UTRA)*; Physical Layer Procedures (3GPP TS 36.213 Version 13.0.0 Release 13); Teesside Small Gauge Railway: Stockton-on-Tees, UK, 2016.
16. GSMA. *3GPP Low Power Wide Area Technologies (LPWA)*; GSMA White Paper; GSMA: London, UK, 2016; p. 19.
17. Semtech. *SX1272 Long Range*; Low Power RF Transceiver 860–1000 MHz with LoRa® Technology; Semtech: Camarillo, CA, USA. Available online: https://www.semtech.com/products/wireless-rf/lora-transceivers/SX1272 (accessed on 26 March 2018).
18. Semtech. *LoRa Family | Wireless and RF ICs for ISM Band Applications*; Semtech: Camarillo, CA, USA. Available online: https://www.semtech.com/products/wireless-rf/lora-gateways (accessed on 26 March 2018).
19. SigFox. *About SIGFOX*; SigFox: Labège, France, 2018. Available online: https://www.sigfox.com/en.
20. Weightless Management Ltd. *Weightless-P Standard Is Designed for High Performance, Low Power, 2-Way Communication for IoT*; Weightless Management Ltd.: Cambridge, UK, 2015. Available online: http://www.weightless.org/news (accessed on 26 March 2018).
21. IEEE Standards Association. *IEEE Std 802.11af–2013 (Amendment to IEEE Std 802.11-2012, as Amended by IEEE Std 802.11ae-2012, IEEE Std 802.11aa-2012, IEEE Std 802.11ad-2012, and IEEE Std 802.11ac-2013)—IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Television White Spaces (TVWS) Operation*; IEEE Standards Association: Piscataway, NJ, USA, 2014.
22. Adame, T.; Bel, A.; Bellalta, B.; Barcelo, J.; Oliver, M. IEEE 802.11ah: The Wi-Fi Approach for M2M Communications. *IEEE Wirel. Commun.* **2014**, 21, 144–152.
23. 5G PPP Architecture Working Group. View on 5G Architecture View on 5G Architecture, 2016. 5G PPP Architecture Working Group. Available online: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-5G-Architecture-WP-July-2016.pdf (accessed on 26 March 2018).
24. Mobile Europe. Verizon Outlines First 5G Radio Specification, 2016. Mobile Europe. Available online: https://www.mobileeurope.co.uk/press-wire/verizon-outlines-first-5g-radio-specification (accessed on 26 March 2018).
25. Verizon 5G Technical Forum. Available online: http://www.5gtf.net (accessed on 26 March 2018).
26. Ericsson, C. *Verizon 5G TF; Network and Signalling Working Group; Verizon 5 th Generation Radio Access; 5G Packet Data Convergence Protocol (5G-PDCP) Specification (Release 1) Document Approvals Name Title Company Date of Approval*; Verizon: New York, NY, USA, 2016.
27. Chávez-Santiago, R.; Szydełko, M.; Kliks, A.; Foukalas, F.; Haddad, Y.; Nolan, K.E.; Kelly, M.Y.; Masonta, M.T.; Balasingham, I. 5G: The Convergence of Wireless Communications. *Wirel. Personal Commun.* **2015**, *83*, 1617–1642.
28. Korhonen, J. 3GPP '5G' Mobility Considerations, 2016. Available online: https://datatracker.ietf.org/meeting/95/materials/slides-95-dmm-0/ (accessed on 26 March 2018).
29. Chakrabarti, S.; Mishra, A. QoS issues in ad hoc wireless networks. *IEEE Commun. Mag.* **2001**, *39*, 142–148.
30. Park, S.; Savvides, A.; Srivastava, M. Simulating networks of wireless sensors. In Proceedings of the 33nd Conference on Winter simulation, Arlington, VA, USA,9–12 December 2001; pp. 1330–1338.

31. Aberer, K.; Hauswirth, M.; Salehi, A. Infrastructure for data processing in large-scale interconnected sensor networks. In Proceedings of the 2007 International Conference on Mobile Data Management, Mannheim, Germany, 7–11 May 2007; pp. 198–205.
32. Akribopoulos, O.; Georgitzikis, V.; Protopapa, A.; Chatzigiannakis, I. Building a platform-agnostic wireless network of interconnected smart objects. In Proceedings of the 15th Panhellenic Conference on Informatics, Kastoria, Greece, 30 September–2 October 2011; pp. 277–281.
33. Thielemans, S.; Bezunartea, M.; Steenhaut, K. Establishing transparent IPv6 communication on LoRa based low power wide area networks (LPWANS). In Proceedings of the Wireless Telecommunications Symposium, Chicago, IL, USA, 26–28 April 2017.
34. Weber, P.; Jäckle, D.; Rahusen, D.; Sikora, A. IPv6 over LoRaWAN™. In Proceedings of the 2016 IEEE 3rd International Symposium on Wireless Systems within the IEEE International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, Manipal, India, 13–16 September 2017; pp. 75–79.
35. Schumacher, C.P.P.; Kushalnagar, N.; Montenegro, G. *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*; IETF: Fremont, CA, USA, 2015.
36. White, G. Active queue management in DOCSIS® 3.1 networks. *IEEE Commun. Mag.* **2015**, *53*, 126–132.
37. Ronan, J.; Walsh, K.; Long, D. Evaluation of a DTN convergence layer for the AX.25 network protocol. In Proceedings of the Second International Workshop on Mobile Opportunistic Networking (MobiOpp '10), Pisa, Italy, 22–23 February 2010; p. 72.
38. Taylor, D.E.; Herkersdorf, A.; Döring, A.; Dittmann, G. Robust header compression (ROHC) in next-generation network processors. *IEEE/ACM Trans. Netw.* **2005**, *13*, 755–768.
39. Conta, A.; Gupta, M. *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*; IETF: Fremont, CA, USA, 2017.